iKSP Journal of Business and Economics
http://iksp.org/journals/index.php/ijbe/index
iKSP Publisher

International Moral Hazard Risks Management in Monetary Institutions

Nizam Shah Allabasc*[1]
[1]University Tun Abdul Razak (UNIRAZAK), Malaysia

Abstract - This study examines moral hazard risk and its impacts on the global monetary industry. While most risks can be attributable to natural causes, moral hazard risks are mainly due to failure of human value systems. The fines which have been imposed on financial institutions have been highlighted by regions, for ease of reference. Measures such as standard operating procedures, robust systems and competent staff together with anti-money laundering (AML) and know your customer (KYC) policies can help control and can prevent, or at least minimise, sanctions and fines. In the case of money laundering, consequences can be severe as it not only destroys local economies but also affects the host economies¬ by financing illegal and terrorism related activities. To prevent AML activities, regulators need to be more aware and stringent in policy implementation Fines and sanctions imposed on financial institutions and the growing nature of such fines and sanctions indicate the severity of this problem in recent times. One way to prevent and/or to reduce this risk is through moral and religious education coupled with adequate regulatory policies, controls and procedures. The implementation of these regulatory policies have to be then monitored and the necessary actions taken to review and enhance them to manage and mitigate any the risks.

Keywords: Moral hazard risk, operational risk, informational technology risk, cyber security risk, digital risk, compliance risk, reputational risk

INTRODUCTION

Risk Management is the process of measuring or assessing the actual or possible hazards of a specific situation. However, there is no major difference in risk management practice in both of the major banking systems. The additional threats that are exceptional to Islamic Banks are through what is known as Shariah Risk. According to Georges Dionne (2013), the aim of a well-defined risk management strategy is to reduce the costs associated with cash flow volatility with a set of financial and operational activities that maximise the value of a company or a portfolio. The universal philosophy of risk management is risk hedging using various instruments, including derivatives and structured products, self-insurance and self-protections and market insurance. Financial distress is one of the main costs that financial institutions and banks seek to minimise, and it includes risk premium to stakeholders, expected income taxes and investment financing. The managers' behaviours in relation to risk aversion and risk appetite, including the overall corporate governance also affects risk management activities. Therefore, key risk categories have been clarified in this study which are generally connected with moral hazard risk. In a study, BCBS (2001) delineates operational risks as the risk of direct and indirect loss resulting from inadequate or failed internal processes, people and systems or from external events.

Reputational Risk refers to possible damage to an administration's reputational wealth. Banks and financial institutions face reputational hazard through various sources, including by financial institution gossips and rumours, actions against the banks, over-eagerness or inadvertent non-compliance with guidelines and regulations or authorities, data manipulations, bad client management service, bad customer experience inside the bank's branches as well as decisions

*Corresponding author:
Email: : nizam_shah@hotmail.com (N.S. Allabasc)
iKSP Journal of Business and Economics (2021) 1(2): 60-65

taken under severe circumstances. Reputational risk can lead to the public losing confidence in the bank. An example of this is the case of Salomon Brothers Inc in the 1990s, which was at that time, the fifth largest investment bank in the United States of America. The bank forged accounts to purchase government securities in quantities much greater than the permissible limits. Lamarque, Eric & Maurer, Frantz (2009), have pointed out that the financial consequences of reputational risk are almost impossible to be calculated precisely and it is not considered to be an operational risk. It was also noted that banking theory has not yet considered reputational risk in its analysis of bank risk management (Iftikhar et al., 2015). This was the principal reason that the bank was able to switch the value that depositors paid for these securities. In 1991, the government caught the bank in its activities resulting in Salomon Brothers suffering significant loss of standing, status and reputation in the United States as well as globally. The United States government charged the bank a total of USD290 million, the biggest fine ever imposed on an investment bank at the time. Another issue is the resistance to Information Technology (IT) Risk Management in financial organisations which carries the potential risk of loss due to, among others, system failures and software designing or programming errors. The prevalence of IT outfits and technology in almost every area of trade and commerce means that most business risks in banking today, from regulatory to reputation, control failures, and IT security risk have a significant IT component. Also, the exposure to these IT related risks has seen an exponential growth with the increase in digital facilities and services provided directly to clients, which consequently, has provided billions of new entry points into bank schemes. However, it has to be noted that when technology risks appear, the monetary, supervisory and reputational consequences can be severe (Mahesar et al., 2014).

Cyber security consists of technologies, processes, procedures and methods that are designed to guard systems, networks, statistics and information from cyber misconducts. It gives entities and industries unique risk identities so as to better organise and network technological systems and also gives them a great deal of awareness about risk management and mitigation. BCBS (2018), describes the diversity of approaches thematically whilst emphasising that this would assist banks and supervisors steer the regulatory environment as well as provide beneficial contribution for recognising ranges where supplementary policy mechanisms could be acceptable. Moving forward, the BCBS Committee proposes to integrate the cyber measurement into its broader operational resilience work. The cyber security operation helps decrease the risk of a cyber-attack and defends entities, organisations and individuals from stealthy manipulation of systems, networks and technologies by sinister entities. However, even the best cyber security is prone to human error. Delvin B. (2016) mentioned in January 2015, a cyber-attack that had been carried out over a period of 10 days, was detected at the Ecuadorian Banco del Austro (BDS) and which resulted in losses of USD12 million. Subsequent investigations found that certain business transactions had irregularities that should have raised doubts among the bank's staff and should have been classified as Cyber Security Risks (Akram et al., 2020). Shariah Risk is exclusive and unique to Islamic banking and financial institutions, and has been sufficiently researched. However, even as regulations have improved, banks still face a challenge in quantifying as well as in mitigating and managing this risk. For Islamic banks, Shariah risk carries potential loss resulting from Shariah non-compliance and improper execution of their fiduciary duties. Together, these risks signify a significant challenge for Islamic banking operations, processes and procedures as well as for stakeholders and require careful identification, mitigation and administration.The unique and exclusive nature of Shariah risk to Islamic banking and financial institutions is because these institutions face certain risks that conventional banks don't, including equity investment risk, displaced commercial risk, rate of return risk and Shariah Non-Compliance Risk. Even as they strive to enhance value for the stakeholders, the board of directors and senior management at these institutions have to take the necessary steps to mitigate and manage these unique risks. In the financial industry, Operational Risk is acknowledged as being as old as banks and could "destroy" any bank, a case in point is that of 223-year-old Barings PLC. Although the basic explanation of operational risk is the risk of loss pursuant to an operational failure, it incorporates a wide range of events and actions by people, systems, processes and external events. Actions by people is referred to as manual or human factor, and includes activities such as, misappropriation of assets, tax evasion, intentional mismarking of positions, corruptions, discrimination, worker's compensation, employee health and safety, theft of information, hacking damage, third party theft and forgery.

Table 1: Banking Operational Risks

	Risk Related		
Nature	**Machine**	**Human**	**Software**
Earthquakes	Maintenance Failure	Oversight	Malware
Fire Accidents	Repairs	Negligence	WannaCry Incidents
Floods	Chemical Threats	Corruption	Hacking
Climate Change	Gas Exposures	Theft and Vandalism	Server Corruption

As shown in Table 1, Banking Operational Risks, which cause disruptions to the business transactions of financial institutions, can be classified in four main categories, namely, Nature, Machine, Human and Software. Nature related risks include earthquakes, fires, floods and any major climatic influence. Machine related risks include machine failure in day-to-day operations, extended repair schedules, chemical threats and gas exposures due to machine malfunctions. Human related risks, on the other hand, include oversight errors, negligence, corruption, theft and vandalism; while software related risks include software issues such as malware, WannaCry incidents, computer hacking and the server corruption.

Additionally, operational risks to financial institutions also includes risks arising, amongst others, from contracts entered not in good faith, where misleading information is provided to induce unjustified risks or about its assets, liabilities or credit capacity and from an effort to produce revenue before a bond's maturity. Then US Federal Reserve Chairman, Bernanke in 2013 discussed the need to make the monetary structure safer and whilst acknowledging the moral challenge that it could pose globally (Bernanke, Ben S. (2013)).

In an article in The Daily Reckoning, Bonner states that Citigroup's Chief Financial Officer, Gary Crittenden recognised that Citi's huge losses and damages publicised in November 2007 were due, among others, to unexpected actions (Bonner, B (2007)). He also points out the record-breaking fines imposed on financial institutions that could be attributable to moral hazard risks and how it still remains as one of the top agenda of regulators globally.

LITERATURE REVIEW

BCBS (2017), postulates that banking standards and supervisory outlooks should be adaptive to new modernisations and innovations while maintaining appropriate policies and standards.

Pascal Golec and Enrico Perotti (2017), stated, among others, that no asset is unconditionally safe. They describe as safe any debt distributed or assured by a safe government, suggesting a country with its own central bank, a steady currency and good defence of assets privileges.

Additionally, Rifaat, Abdel & Simon (2013) elucidated the importance of an area of regulation that has brought attention to operational risk due to cases of operational risk failure in financial institutions namely the failure in risk oversight by Senior Management in relation to proper implementation of the relevant auditing and accounting practices which have manifested themselves in different activities of these banks and financial institutions.

Then US Federal Reserve Chairman, Bernanke in 2013 discussed the need to make the monetary structure safer and whilst acknowledging the moral challenge that it could pose globally (Bernanke, Ben S. (2013)

A paper by Donnellan & Rutledge (2016) discussed agency cost theory for certain operational risks that arose as a consequence of the 2007 monetary crisis, one of the worst financial catastrophe in two generations, which caused banks to suffer severe credit and liquidity pressure in the USA and finally resulting in the government formulating new financial strategies to help steady the finance and related businesses.

METHODOLOGY

All statistics and information were collected from reliable countrywide summary sources and cross referenced against regulator-maintained websites wherever accessible. The fines and activities from various authorities and jurisdictions with high cross border monetary trades were comprised in this study. Authorities, jurisdictions and agencies that have significantly less volume of fines and penalties, and that were also less forceful in their execution of the same, were not included in this study as they did not affect the trends meaningfully. The data collection and source of information is from Fenergo (2018), which provides global regulatory compliance technologies.

Findings and Implications

Since the start of the global monetary crisis in 2008, global banks and financial institutions have had to contend with an increasing series of guidelines and regulations meant to ensure clarity and transparency in a bid to produce safer, robust and more see-through monetary arrangements and systems. Fenergo (2018) has complied an extensive record of financial penalties levied by international regulators against banks and financial institutions with respect to AML, KYC and other regulation related sanctions. As noted, global financial institutions have been fined a staggering USD26 billion for AML, sanctions and KYC non-compliance in the last decade.

Nor Shamsiah, a regulator in Malaysia has executed many policies, guidelines and enforcements to help protect the local financial system against money laundering and terrorism financing related risk. As stated, Banking and Financial Institutions, as corporate citizens, have a responsibility to play their part in safeguarding the economy and the monetary system. Table 2 shows the breakdown of global AML Fines by region from 2008 to 2018 and helps process the monetary impact that these fines have had on global banks and financial institutions over these ten years. It records the activities of regulators across the North American, European, Asia Pacific (APAC) and Middle East (ME) regions. The main findings from this research indicate that global regulators are increasingly putting banks and financial institutions' AML

and KYC terms of references, policies, procedures and technologies under micro level views on both the administrative and supervisory level.

Mahathir Mohamad has mentioned that, for Malaysia to be transformed into a value-driven developed nation, everybody needs to play their part in the fight against financial crime and that shared prosperity could only be achieved through shared responsibility (Tun Dr Mahathir Bin Mohamad (2019)). He went on to say that both financial institutions as well as all citizens had a vital role to play in preserving the integrity of Malaysia's economic system.

Inadequate customer risk profiling, insufficient customer due diligence controls and the lack of consistent follow-ups in global AML compliance programs were commonly cited as the principal failings of penalised organisations. As for sanctions violations, erroneous screening processes and procedures, false hits and overlooked red flag tags in the systems by sanctioned organisations was a frequent refrain in the study. According to Tom Groenfeldt (2018), between 2009 and 2012 more than 50,000 regulations and guidelines were published across the G20 (Group of 20) nations, with almost 50,000 supervisory updates being made in 2015 alone.

Table 2: Global AML Fines by Region 2008 to 2018 Breakdown

No	Region	USD Amount Levied
1	North American	23,560,300,113.00
2	European	1,703,958,787.00
3	APAC	608,512,772.00
4	ME	9,446,600.00
Total		25,882,218,272.00

Source: Fenergo, Dublin-Ireland (2018)

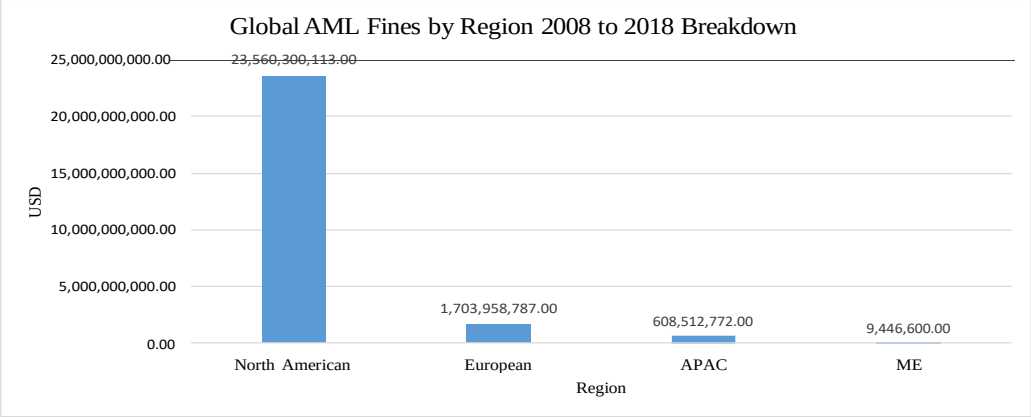

Figure 1: Global AML Fines by Region 2008 to 2018 Breakdown (*Source: Fenergo, Dublin-Ireland, 2018)*

Figure 1, which represents a breakdown of global AML fines by region from 2008 to 2018, shows that on a regional level, the United States (US) had levied 91% of all global AML, KYC and sanctions related fines totalling USD23.56 billion during this period. Globally, the US Department of Justice (DOJ) accounted for the highest number of enforcement actions imposed during this 10-year period.

During this period, Europe issued fines, totalling USD1.7 billion, with most of it being imposed by the UK's Financial Conduct Authority (FCA). Financial Conduct Authority, (2018) provides for sanctions that are regulatory or governmental orders that prohibit a firm from carrying out transactions with a sanctioned person or organisation, and in some cases prohibit a firm from providing any financial services at all to these entities.

2018 has also been a record year for AML penalties in the region, totalling USD903 million, with the maximum European AML penalties of this 10-period totalling USD900 million imposed by the Dutch authorities. BCBS (2019), references third party developers' involvement in system designs and suggests that banks and their supervisors should pay particular attention and enforce strict due diligence to the challenges posed by the increased sharing of customer-permissioned data coupled with the need for enhanced connectivity among the various financial services.

AML related penalties totalling USD609 million have been issued in the APAC region during this 10-year period, with 2018 heralding a new 10-year record for enforcement with nearly USD541 million issued in penalties during the first eight months of the year. This also includes the largest penalty levied in Australian business history. The 1Malaysia Development Berhad (1MDB) scandal has heightened world-wide attention on this problem and has contributed to greater administrative and enforcement activity since 2016. Additionally, Singaporean and Hong Kong regulators, in an

endeavour to protect their financial institutions, have issued guidelines and regulations in a bid to prevent or mitigate any AML, KYC and related violations.

Alexandra Rosi (2015), has suggested that some banks and financial institutions seem to be purposefully de-risking their client portfolio by terminating accounts of Politically Exposed Persons (PEPs) due to the increased resource and compliance costs associated with reviewing and continuing these relationships. This has been caused by, among others, crude rules based on very simple matching criteria, that have been plotted against uncleansed customer data, imperfect list records, unexpected changes to sanctions lists, poorly designed and formatted customer information data, misspellings, aliases and possible growth in third party references lists.

In the Middle East region, which has a less robust supervisory administration, regulators are in the preliminary stages of fine-tuning their guidelines in an effort to combat AML, KYC and related wrongdoings. The Dubai Financial Services Authority (DFSA) has been the most active regulator in the zone, imposing penalties totalling USD9.5 million for AML breaches. In addition, Ion Croitoru (2014) explained that the exposure to operational risk in organisations could have an upward or downward risk appetite depending on the volume and complexity of transactions carried out as well as the quality and reliability of systems used in the internal control systems implemented. Therefore, all risks associated objectives, activities or actions taken should, as far as possible, be identified and recorded.

CONCLUSION

As can be seen from the data above for the period from 2008 to 2018, international supervisory and regulatory entities have had to proactively enforce AML regulations and executions efficiently and competently to prevent money laundering and counter financing of terrorism related activities. This change in attitude can be seen in the unprecedented number of financial penalties levied by regulatory agencies, especially in the United States of America.

Between 2012 and 2015, nearly 90% of all penalties levied were pertaining to Banking Secrecy Act and AML related transgressions, compared to less than half from 2002 through to 2011. In 2015 alone, global sanctions and penalties related to AML contraventions amounted to USD11.5 billion. Although, basing on statistics from the past 3 years, there seems to be a flattening of this trend, banking and financial institutions have to continue to heed and implement the relevant regulatory guidelines to prevent and protect against any losses connected to financial, moral and/or reputational risks.

For banking and financial institutions, the main concern should be risk management along with compliance with and execution of all relevant regulatory guidelines and any revisions thereto. It should be of utmost importance even as banks and financial institutions strive for growth and new client engagements. Conveying awareness and understanding of customer needs through good compliance practices, enhancement of monetary and administrative skills as well as employing up-to-date technologies will help banks and financial institutions stay ahead of the industry.

Additionally, banking and financial institutions should have in place and implement sufficient control measures to help mitigate AML risks of any customers identified in the risk assessment stage by having adequate policies, controls and procedures to manage and minimise any risks that have been identified. This then has to be followed by monitoring and implementing those policies, controls and procedures, reviewing and enhancing them, if necessary, in addition to taking enhanced measures to manage and mitigate the risks where higher risks have been identified.

To further enhance the operational and moral hazard risk management and to lessen any penalties, the monetary industry worldwide is now embracing and implementing new technologies such as Artificial Intelligence (AI), electronic KYC (eKYC) via facial recognition, Robotics Process Automation (RPA) and smartphone applications to create a single platform for understanding and engaging with clients.

Acknowledgement

The author research titled a robust comparison among Islamic and conventional banks' on operational risks management and this journal was presented virtually in International Conference on Innovative Trends in business and Technology (iCITBT 2020) and supported by MyBrain15, which is a program introduced by the Malaysian Ministry of Higher Education (MOHE) which finances postgraduate student's education.

REFERENCES

Akram, F., Abrar ul Haq, M., Natarajan, V. K., & Chellakan, R. S. (2020). Board heterogeneity and corporate performance: An insight beyond agency issues. *Cogent Business & Management*, *7*(1), 1809299.

Alexandra Rosi (2015), How to Audit Controls to Manage Financial Crime Compliance (FCC) Risks Associated with Politically Exposed Persons, Association of Certified Anti-Money Laundering Specialist (ACAMS), USA. Retrieved from: http://www.acams.org/wp-content/uploads/2015/08/How-to-Audit-Controls-to-Manage-FCC-Risks-Associated-with-PEPs-A-Rosi.pdf

BCBS (2001). *Operational Risk, Working Paper,* Bank for International Settlement.

BCBS (2017), Implications of Fintech Developments for Banks and Bank Supervisors. Basel Committee on Banking Supervision (*BCBS*), Bank for International Settlements, Basel, Switzerland. Available at: <https://www.bis.org/bcbs/publ/d415.htm > [Accessed 15th December 2020]

BCBS (2018), Cyber-resilience: range of practices. Basel Committee on Banking Supervision (*BCBS*), Bank for International Settlements, Basel, Switzerland. Available at: <https://www.bis.org/bcbs/publ/d454.htm> [Accessed 15th December 2020]

BCBS (2019), Consolidated Basel Framework. Basel Committee on Banking Supervision (*BCBS*), Bank for International Settlements, Basel, Switzerland. Available at: < https://www.bis.org/bcbs/publ/d462.htm> [Accessed 15th December 2020]

Bernanke, Ben S. (2013), Communication and Monetary Policy, speech delivered at the National Economists Club Annual Dinner, Herbert Stein Memorial Lecture, Washington, D.C., on 19th November 2013.

Bonner, B. (2007). Goldman Sachs was Wrong and 2 Million Families May Lose Their Homes, retrieved from: http://www.dailyreckoning.com.au/goldman-sachs-3/2007/11/14/ [Accessed 15th December 2020]

Devlin Barret, Katy Burne (2016), Now It's Three: Ecuador Bank Hacked via Swift. The Wall Street Journal. Dow Jones & Company, Inc. Retrieved from: https://www.wsj.com/articles/lawsuit-claims-another-global-banking-hack-1463695820 [Accessed 15th December 2020]

Fenergo (2018), Global Financial Institutions Fined $26 Billion for AML, Sanctions & KYC Non-Compliance, Dublin, Ireland, Retriever from: https://www.fenergo.com/press-releases/global-financial-institutions-fined-$26-billion-for-aml-kyc.html [Accessed 15th December 2020]

Financial Conduct Authority (2018), Financial Sanctions, London United Kingdom, Retrieved from: https://www.fca.org.uk/firms/financial-crime/financial-sanctions [Accessed 15th December 2020]

Georges Dionne (2013), Risk Management; History, Definition and Critique, Interuniversity Research Centre on Enterprise Networks, Logistics and Transportation (CIRRELT) and Department of Finance, Canada.

Iftikhar Ahmad, Aneel Rahim, Adeel Javed, Hafiz Malik. (2015). Security of Information and Networks. *The Scientific World Journal*, 2015, Article ID 150640, 2 pages,. https://doi.org/10.1155/2015/150640

Ion Croitoru, (2014), Operational Risk Management and Monitoring, Internal Auditing and Risk Management, Athenaeum University of Bucharest, Vol. 36(1), Pages 21-31, December 2014.

John T. Donnellan & Wanda Rutledge (2016), Agency Theory in Banking - 'Lessons from the 2007-2010 Financial Crisis'. International Journal of Business and Applied Social Science Vol.2, No.3, March, 2016. School of Business, New Jersey City University, Jersey City, USA. Available at: < file:///E:/Downloads/56fcac803a86011459399808.pdf> [Accessed 15th December 2020]

Lamarque, Éric, Maurer, Frantz, (2009). *Operational Risk in Banks: Designing A Supervision and Control Framework*, French Journal of Management. February 2009, Issue 191, p93-108.

Mahathir Bin Mohamad (2019), Special Address by Prime Minister of Malaysia at The 11th International Conference On Financial Crime and Terrorism Financing (IFCTF) 2019 Building Trust and Transparency: Collaborate, Accelerate, Strengthen On 5 November 2019, Malaysia. Access: https://www.pmo.gov.my/wp-content/uploads/2019/11/Media-Copy-Special-Address-by-YAB-PM-at-the-11th-IFCTF-2019-on-5-November-2019-1.pdf [Accessed 15th December 2020]

Mahesar, A. W., Malik, H. A. M., Ahmad, A., Shah, A., & Wahiddin, M. R. (2014, November). Calculus and its applications in scale-free networks. In *The 5th International Conference on Information and Communication Technology for The Muslim World (ICT4M)* (pp. 1-6). IEEE.

Nor Shamsiah Mohd Yunus (2019), Key Address by Governor of Central Bank of Malaysia at The 11th International Conference On Financial Crime and Terrorism Financing (IFCTF) 2019 Building Trust and Transparency: Collaborate, Accelerate, Strengthen On 5 November 2019, Malaysia. Access: https://www.bnm.gov.my/index.php?ch=en_speech&pg=en_speech&ac=842 [Accessed 15th December 2020]

Pascal Golec and Enrico Perotti, (2017), Safe assets: a review, No 2035, Working Paper Series, European Central Bank; Frankfurt a. M. Available at: https://www.ecb.europa.eu/pub/pdf/scpwps/ecbwp2035.en.pdf [Accessed 15th December 2020]

Rifaat Ahmed, Abdel Karim, Simon Archer, (2013). *Islamic Finance: The New Regulatory Challenge*, (2nd Edition), Published by John Wiley and Sons, Singapore Pte Ltd., Page 134 to 151.

Tom Groenfeldt (2018), Taming The High Costs of Compliance with Tech, Forbes Media, USA Access: https://www.forbes.com/sites/tomgroenfeldt/2018/03/22/taming-the-high-costs-of-compliance-with-tech/#796acec55d3f